An Introduction to Enterprise Digital Rights Management

SECLORE™

The Reality: Sensitive Information Flows Unprotected Beyond the Organizational Perimeter Every Minute

Every day, your employees share sensitive business information internally and with numerous external collaborators. And while your organization's success often depends on such collaboration activities, data leakage can quickly occur since the information typically leaves your enterprise perimeter unprotected.

Likely, you need to know what is happening to your information, particularly who is using (or misusing) the data after it leaves your organization. However, once information exits the organization, you cannot control who can access the data. Additionally, your employees may also leak data accidentally or sometimes maliciously. Now, your enterprise is liable to face severe risks: regulatory, legal, reputational, and financial.

Consider the following common scenarios:

- Accessing and downloading documents onto laptops and mobile devices, which, when lost, form the largest source of data breaches worldwide.
- Sharing sensitive information with vendors, partners, and other third parties, where it is at the highest risk of being stolen, sold, or lost.
- Using cloud-based services (Dropbox, Google Drive, etc.) for sharing files, where the information is spread across various legal jurisdictions.
- Relying solely on NDAs to secure your Intellectual Property (IP) as a reactive measure instead of a proactive one.

Enabling Collaboration Without Sacrificing Data Security: A New Approach

In today's digital world, collaboration is essential for businesses of all sizes. However, collaboration can also pose a security risk if not done correctly. When multiple people have access to the same data, it is more likely to be compromised. Generally, it is advisable for organizations to consider the following measures when enabling collaboration without sacrificing data security:

Be aware of the risks

Before you start collaborating, you must be aware of the risks involved. These risks include data breaches, unauthorized access, and data loss.

Choose the right tools

There are many different tools available for collaboration. It is essential to choose the right tools for your needs and ensure they are secure.

Educate your users

Your users need to be aware of the security risks involved in collaboration. They also need to know how to use the tools securely.

Monitor your activity

Monitoring your collaboration activity to detect suspicious behavior and quickly identify and respond to security threats is essential.

How Does Seclore Data-Centric Security Help?

A data-centric approach starts by directly embedding security and usage policies into the data. Unlike traditional perimeter-based defenses, this approach ensures that the data forms its security boundary, regardless of where it travels, how it is accessed, or who is attempting to access it. The embedded security measures remain in effect whether the data is being shared as email attachments or accessed through file shares, cloud collaboration platforms, thumb drives, or other means.

Seclore data-centric security ensures the following:

Knowledge of Sensitive Data	Understanding where the organization's data lies and how it moves across various touchpoints within and outside the organization.
Compliance	Addressing compliance requirements stipulated by various data protection laws worldwide like GDPR, CCPA, EAR-ITAR, SDAIA, IRDAI Cybersecurity Guidelines, etc.
Purpose and Storage Limitation	Limiting the usage and storage of data by stating specific rules to access and utilize data, along with providing a way to destroy the data after accomplishing the objective.
Audit Trail	Enhance an organization's accountability, integrity, and confidentiality stance by allowing it to track and audit sensitive data and ensure that it doesn't fall prey to unauthorized access.

Securing Information Wherever It Goes

Your data is in constant motion. The proliferation of intelligent devices and cloud technologies enables employees and partners to access enterprise data from anywhere. It's out of control once it leaves your enterprise — whether shared with a trusted third party or leaked. We call this the data security gap and are trying to fix it.

Prevent Data Theft & Achieve Compliance

Know	Protect	Control
Exactly what's shared and where your data is	**Every single asset wherever it goes**	**Who has access and revoke it at any time**
• Risk insights & trends • Access patterns & usage analytics • Location awareness	• Policy management • Dynamic watermarking • Classification labeling • AES256 bit encryption	• Granular access control • Real-time access revocation • Dynamic policy federation

Seclore's comprehensive enterprise digital rights management empowers you to know, protect, and control your valuable information, safeguarding it from unauthorized access and potential breaches. With Seclore data-centric security, organizations can:

- **Know** which assets are sensitive and where they are in the organization.
- **Protect** the data using digital asset classification, dynamic watermarking, and AES256-bit encryption.
- **Control** and track access to sensitive digital assets using granular usage controls and risk insights dashboards.

Extending Data-Centric Security to Collaboration Solutions

Many organizations use document management systems such as Enterprise Resource Planning (ERP), Enterprise Content Management (ECM), and Document Management Systems (DMS) to store and manage the organization's sensitive Intellectual Property (IP).

Using these systems, you provide access to different areas/libraries/folders to restrict only data access to authorized users. However, all security and control are lost once these users (employees or third-party users) download or extract the information from these systems as stand-alone files.

Seclore Enterprise Digital Rights Management (EDRM) enables organizations to integrate with their existing data management systems consisting of and automate the end-to-end data-centric security process.

Using Seclore Enterprise Digital Rights Management (EDRM), organizations can:

- **Maintain clean records of all data:** Enable organizations to maintain a complete audit trail of the time, location, and other details of the activities performed on the content, updated in real-time.
- **Dynamically update or revoke permissions:** Allow organizations to update usage policies across all document copies remotely and allows you to remove access when a project reaches completion or an employee exits.
- **Enable easy authentication for external users:** Seamless identity federation with the various sources of Single Sign-on (SSO), social media, and directory sources to enable authorized users to access sensitive data in a secure environment.

Protect and Control Your Information – Anytime, Anywhere

Many Fortune 500 companies across the world are utilizing Seclore's technology. Seclore is trusted and used by organizations such as Linde Engineering, Panasonic, GE, the Reliance Group, Fugro, the Essar Group, and many more.

Seclore's data-centric security platform has constantly enabled organizations to:

- Protect their confidential information and intellectual property.
- Comply with the relevant guidelines and regulatory compliance obligations.
- Eliminate data leakage and theft, especially while outsourcing business operations or during cross-enterprise collaboration.

Collaboration Applications	SharePoint, OneDrive, Teams, box, SAP
Email	Outlook
DLP	Forcepoint, BROADCOM
CASB	Skyhigh Security
Classification solutions	Microsoft Sensitivity Labels

Seclore on Mobile: Seclore ensures that access and usage controls are automatically attached to sensitive emails and documents when sent. When authorized users open a protected email on a mobile device or MDM application, they can view, edit, and save the saved document and reply securely in email.

Seclore supports all kinds of mobile platforms. However, the following out-of-the-box solutions include:

- Seclore for iOS
- Seclore for Android
- Seclore for MDM/EMM solutions

Seclore APIs: Seclore offers a robust collection of APIs and rapid configuration capabilities that reduce the effort required to add persistent, granular usage controls and tracking information as it is discovered, downloaded, classified, and shared.

- Documentation protection
- Documentation inspection
- Policy federation
- Secure online rendering

Conclusion

Seclore Enterprise Digital Rights Management is a powerful and versatile solution that can help organizations to protect their sensitive data. It offers several features that make it a valuable tool for data security, and it can be integrated with other systems to automate the protection of your data.

Additionally, Seclore EDRM offers benefits such as compliance with GDPR, CCPA, and SDAIA Regulations and scalability to allow organizations to expand their data security with their growth.

Seclore is the world leader in data-centric security and has helped over 1,000 companies across a wide range of the most sensitive industries (financial services, manufacturing, public sector, telecom, etc.) successfully transition to this new model. By implementing new concepts pioneered by Seclore, these companies have protected their data, achieved regulatory compliance, and eased collaboration friction without fear.

SECLORE™

About Seclore

Protecting the world's sensitive data wherever it goes. Seclore protects and controls digital assets to help enterprises close their data security gap to prevent data theft and achieve compliance. Our data-centric approach to security ensures that only authorized individuals have access to sensitive digital assets, inside and outside of their organization. Enterprises can set automated policies and enable users to control and revoke who has access, what access they have, and for how long. Learn why leading enterprises like American Express and Applied Materials choose Seclore to protect and control their digital assets without sacrificing seamless collaboration and data sharing.

Visit **www.seclore.com** for more information.

5201 Great America Parkway
Suite 440
Santa Clara, CA 95054